Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (previously presented): A cryptographic method for a transaction whereby a first entity generates, by means of an RSA private key, a proof verifiable by a second entity by means of an RSA public key associated with said private key, said public key comprising a public key exponent and a modulus, the method comprising the steps of:

generating, at the first entity, a first element of proof by using a generic number raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the first entity, whereby calculation of said first element of proof is executable independently of the transaction;

generating, at the first entity, a second element of proof related to the first element of proof and dependent on a common number shared by the first and second entities specifically for the transaction; and

verifying, at the second entity, that the first element of proof is related through a relationship with a second power, modulo the modulus, of a generic number having a second exponent equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof.

Claim 2 (currently amended): The cryptographic method as claimed in claim 1, wherein, for identifying the first entity, the first element of proof is generated by the first entity by raising the generic number to a first power modulo the modulus having a first exponent equal to the ~~pubic~~ public key exponent multiplied by a random integer kept secret by the first entity,
wherein the common number is chosen randomly from within a security interval [0,t 1] and then sent by the second entity after having received the first element of proof, and
wherein the relationship verified by the second entity is an equality relationship between a power of the first element of proof and the first power of the generic number.

Claim 3 (previously presented): The cryptographic method as claimed in claim 1, wherein for signing a message, the first element of proof is generated by the first entity by applying a hash function to the message and to the generic number, raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the first entity, wherein the common number is equal to the first element of proof, and
wherein the relationship verified by the second entity is an equality relationship between the first element of proof and a result of said hash function applied to the message and to the first power of the generic number.

Claim 4 (previously presented): The cryptographic method as claimed in claim 1, wherein for authenticating that a message received by the second entity comes from the first entity, the first element of proof is generated by the first entity by applying a hash function to the message and to the generic number raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the first entity,
wherein the common number is chosen at random from within a security interval [0,t 1] and then sent by the second entity after having received the first element of proof, and
wherein the relationship verified by the second entity is an equality relationship between the first element of proof and a result of said hash function applied to the message and to the first power of the generic number.

Claim 5 (previously presented): The cryptographic method as claimed in claim 4, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number,
wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and
wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.

Claim 6 (previously presented): The cryptographic method as claimed in claim 4,

wherein the common number comprises first and second elementary common numbers,

wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number,

wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof,

and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number.

Claim 7 (previously presented): The cryptographic method as claimed in claim 6, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 8 (previously presented): The cryptographic method as claimed in claim 6, wherein the random number is greater than the value of the private key in relation to a mathematical problem of a discrete logarithm.

Claim 9 (previously presented): The cryptographic method as claimed in claim 7, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 10 (previously presented): The cryptographic method as claimed in claim 9, wherein the first exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 11 (previously presented): The cryptographic method as claimed in claim 1, wherein the generic number is transmitted with the public key, the generic number being equal to a simple number raised to a power modulo the modulus with the private key as exponent.

Claim 12 (previously presented): The cryptographic method as claimed in claim 1, further comprising the steps of:

receiving the second element of proof at a third entity;

generating a third element of proof at the third entity by raising the generic number to a power, modulo the modulus, with the second element of proof as exponent;

sending the third element of proof to the second entity; and

at the second entity, raising the third element of proof to a power of the public key exponent, modulo the modulus, multiplying the result thereof by the generic number raised to a power whose exponent is the common number in order to verify the relationship relating the first element of proof to the second element of proof.

Claim 13 (previously presented): A prover device having an RSA private key kept secret and protected against intrusions, for generating, during a transaction with a verifier device, a proof whose verification by means of a public key associated with said private key ensures that said prover device has originated said proof, said RSA public key comprising a public key exponent and a modulus, the prover device comprising:

calculation means for generating a first element of proof completely or partly independently of the transaction, said first element of proof being generated by said prover device by raising a generic number to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer kept secret by the prover device, and for generating a second element of proof related to the first element of proof and dependent on a common number specific to the transaction; and

communication means for transmitting at least the first and second elements of proof and for transmitting said common number to the verifier device or receiving said common number from the verifier device.

Claim 14 (previously presented): The prover device as claimed in claim 13,

wherein the calculation means is, on the one hand, designed to generate a first random number and to raise a generic number to a first power, modulo the modulus, having a

first exponent equal to the first exponent of the public key multiplied by the random integer; and

wherein the calculation means is, on the other hand, designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number or, where the common number is split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number.

Claim 15 (previously presented): The prover device as claimed in claim 14, wherein the calculation means is designed to carry out operations modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 16 (previously presented): A verifier device for verifying that a proof originates from a prover device provided with an RSA private key kept secret by the prover device, by means of a public key associated with said private key, said RSA public key comprising a public key exponent and a modulus, the verifier device comprising:

communication means for receiving a first element of proof, which includes at least the result of a first power, modulo the modulus, of a generic number raised to the power of a first exponent equal to the public key exponent multiplied by a random integer, and a second element of proof or a third element of proof, and for receiving or transmitting a common number specific to a transaction within which the first and the second or the third element of proof are received; and

calculation means for verifying that the first element of proof is related through a relationship, modulo the modulus, with a second power of the generic number having a second exponent equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof.

Claim 17 (previously presented): The verifier device as claimed in claim 16, wherein the communication means is designed to receive the second element of proof and wherein the calculation means is designed to calculate the second exponent and said second power of the generic number.

Claim 18 (previously presented): The verifier device as claimed in claim 16, wherein the communication means is designed to receive the third element of proof and wherein the calculation means is designed to raise the third element of proof to a power of the public key exponent in order to multiply the result thereof by the generic number raised to a third power having the common number as exponent.

Claim 19 (previously presented): The cryptographic method as claimed in claim 2, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent - multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.

Claim 20 (previously presented): The cryptographic method as claimed in claim 19, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 21 (previously presented): The cryptographic method as claimed in claim 20, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 22 (previously presented): The cryptographic method as claimed in claim 19, wherein the first exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 23 (previously presented): The cryptographic method as claimed in claim 3, wherein the second element of proof is generated by the first entity by subtracting, from the random integer, the private key multiplied by the common number, wherein the linear combination equal to the second exponent comprises a positive unitary coefficient for the common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with a unitary exponent power.

Claim 24 (previously presented): The cryptographic method as claimed in claim 23, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 25 (previously presented): The cryptographic method as claimed in claim 24, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 26 (previously presented): The cryptographic method as claimed in claim 23, wherein the first exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 27 (previously presented): The cryptographic method as claimed in claim 2, wherein the common number comprises first and second elementary common numbers, wherein the second element of proof is generated by the first entity by subtracting, from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number, wherein the linear combination equal to the second exponent comprises a zero coefficient for the first elementary common number, a positive unitary coefficient for the second elementary common number and a positive unitary coefficient for the public key exponent multiplied by the second element of proof, and wherein, in the verified relationship, the first element of proof is considered with an exponent power equal to the first elementary common number.

Claim 28 (previously presented): The cryptographic method as claimed in claim 27, wherein the second element of proof is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.

Claim 29 (previously presented): The cryptographic method as claimed in claim 28, wherein the random integer is less than an image of the modulus via a Carmichael function or less than a multiple of the order of the generic number modulo the modulus.

Claim 30 (previously presented): The cryptographic method as claimed in claim 27, wherein the first exponent is calculated modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus.